Universitair Informatiemanagement

UNIVERSITEIT TWENTE.

Kenmerk: SB/UIM/15/0106/khv
Datum: 7 december 2015

Status: Definitief
Datum vastgesteld in CvB: 7-12-2015
Auteur: Wim Koolhoven

Informatiebeveiligingsbeleid Universiteit Twente

Samenvatting 2

1 Inleiding 3

1.1 Reikwijdte van het beleid 3
1.2 Aanleiding 3
1.3 Korte historie 4
1.4 Leeswijzer 4

2 Doelstelling informatiebeveiligingsbeleid 5

3 Uitgangspunten informatiebeveiliging 6

3.1 Basisregels 6
3.2 Beleidsuitgangspunten 6
3.3 Classificatie 7

4 Governance informatiebeveiligingsbeleid 8

4.1 Afstemming met aanpalende beleidsterreinen 8
4.2 Documenten 8
4.3 Organisatie van de informatiebeveiligingsfunctie 8
4.4 Naleving en bewustwording 10

5 Melding en afhandeling van incidenten 11

Bijlage A Wetgeving 12

Bijlage B Beleidsdocumenten 14

Bijlage C Securityregels 15

Securityregels – Authenticatiemiddelen 16
Securityregels – Basis ICT-voorzieningen 17
Securityregels – Datacentra 18
Securityregels – Hardware 19
Securityregels – Informatiesystemen 20
Securityregels – Netwerk 21
Securityregels – SIEM (Security Incident- en Eventmanagement) 22
Securityregels – Werkplekken 23

Het informatiebeveiligingsbeleid Universiteit Twente is gebaseerd op het Model Informatie-beveiligingsbeleid van het Hoger Onderwijs opgesteld door SURFibo[1] en gepubliceerd onder de Creative Commons[2] licentie.

Samenvatting

Beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening zijn van groot belang. Hoe we deze aspecten op de UT borgen wordt vastgesteld in dit beleid. Het belang van informatiebeveiliging blijkt ook uit het rapport Cyberdreigingsbeeld[3] van SURF.

De UT houdt zich aan de wet en informatie over studenten en medewerkers wordt zo zorgvuldig als mogelijk behandeld. Aandacht hiervoor hoort bij de proactieve houding van iedere medewerker, tegelijkertijd worden er niet meer maatregelen genomen dan noodzakelijk om het ondernemende en creatieve karakter van de UT niet te frustreren.

Informatiebeveiliging is ieders verantwoordelijkheid en een lijnverantwoordelijkheid. Leidinggevenden dragen de primaire verantwoordelijkheid voor een goede informatiebeveiliging op hun afdeling / eenheid. Alle informatiesystemen worden geclassificeerd op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid; deze classificatie bepaalt het niveau van de beveiligingsmaatregelen.

De verantwoordelijkheid van alle betrokken functionarissen wordt beschreven. In het bijzonder van de security officer, security manager, systeemhouders en leidinggevenden. Het belang van het regelmatig onder de aandacht brengen van beveiligingsrisico's en –maatregelen wordt uitgewerkt. De rol van CERT-UT (Computer Emergency Response Team UT) wordt vastgelegd.

Om bewustwording en gedragsbeïnvloeding van medewerkers en studenten met betrekking tot informatiebeveiliging en privacy te bewerkstelligen wordt vanuit Universitair Informatiemanagement een werkgroep ingesteld.

In de bijlagen wordt ingegaan op de relevante wetgeving, wordt een overzicht gegeven van de overige beleidsdocumenten en gedragscodes op het gebied van informatiebeveiliging en worden de securityregels (operationele richtlijnen) geformuleerd.

[1] Informatiebeveiligers en privacy officers werkzaam in het hoger onderwijs overleggen in SCIPR (SURF Community voor Informatiebeveiliging en PRivacy, voorheen SURFibo). Het doel is de informatie-beveiliging en privacy bij hogescholen en universiteiten te verbeteren. Dit doet SCIPR o.a. door het ontwikkelen van beleid en leidraden.
[2] zie http://creativecommons.org/licenses/by/3.0/nl/
[3] Rapport Cyberbedreigingsbeeld Sector Hoger Onderwijs en Wetenschappelijk Onderzoek https://www.surf.nl/kennis-en-innovatie/kennisbank/2014/rapport-cyberbedreigingsbeeld-sector-hoger-onderwijs-en-wetenschappelijk-onderzoek.html

1 Inleiding

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen. Hierbij gaat het ook om de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van de Universiteit Twente. In de bedrijfsvoering, maar ook in het onderwijs en onderzoek is sprake van toenemende afhankelijkheid van informatie en computersystemen, waar kwetsbaarheden en risico's kunnen optreden. Het is daarom van belang hiertegen adequate maatregelen te nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en onderzoek en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoverlies.

De Universiteit Twente heeft de ambitie om met het onderhavige beleidsdocument informatie-beveiliging structureel naar een hoger niveau te brengen en daar te houden door de aspecten governance, wet- en regelgeving, de organisatie van de beveiligingsfunctie en het informatiebeveiligingsbeleid – ook in hun onderlinge relatie – duidelijk te beschrijven en vast te stellen. Privacy krijgt op de UT steeds meer aandacht en de wetgeving wordt stringenter. Eind 2015 wordt er een apart privacybeleid opgesteld.

1.1 Reikwijdte van het beleid

Bij de Universiteit Twente wordt informatiebeveiliging breed geïnterpreteerd. Er is een nauwe relatie en een gedeeltelijke overlap met aanpalende beleidsterreinen, zoals safety (ARBO- en milieuwetgeving), fysieke beveiliging en business continuity. In het kader van "integrale veiligheid" is een goede afstemming tussen deze aanpalende beleidsterreinen nodig.

Het informatiebeveiligingsbeleid binnen de Universiteit Twente heeft betrekking op alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur / outsourcing), alsmede op alle organisatieonderdelen. Tevens vallen onder het informatiebeveiligingsbeleid alle devices waarmee geautoriseerde toegang tot het instellingsnetwerk verkregen kan worden.

Bij het informatiebeveiligingsbeleid ligt de nadruk op de informatie en toepassingen die vallen onder de verantwoordelijkheid van de Universiteit Twente.

1.2 Aanleiding

Het huidige Informatiebeveiligingsbeleid is verouderd en wordt onvoldoende gekend en gedragen in de organisatie. In 2012 en in 2013 heeft de UT meegedaan aan de SURFaudit. Het resultaat geeft inzicht in het volwassenheidsniveau van de UT op het gebied van informatiebeveiliging en privacybescherming. Begin 2015 heeft het CvB besloten[4] om het ambitieniveau hiervoor vast te stellen op minstens volwassenheidsniveau 3: Defined Process. De UT bevindt zich nog niet op het gewenste niveau (deels op niveau 1 of 2). Het ontbreekt voornamelijk aan bewustzijn en juist gedrag.

De bestaande security policies zijn in de loop van 2007 – 2008 ontwikkeld en in 2009 vastgesteld. Om te toetsen of een actualisatie noodzakelijk is, zijn deze eind 2013 door ICTS geëvalueerd. Hierbij is geconcludeerd dat de beheerders weliswaar op de hoogte zijn van het bestaan van de policies, maar de inhoud onvoldoende kennen en nieuw ingerichte diensten niet tegen de policies worden getoetst. Verder werd geconcludeerd dat de policies niet aansluiten bij de terminologie en werkwijze van ICTS.

[4] Ambitieniveau SURFaudit, kenmerk SB/UIM/14/0902/khv, zie https://www.utwente.nl/uim/informatiebeveiliging/ambitieniveau-surfaudit.pdf

1.3 Korte historie

Na de instelling van informatiemanagement is in 2008, tegelijk met het Informatie- en ICT-plan UT 2008-2010 ook een nieuw Informatiebeveiligingsbeleid Universiteit Twente vastgesteld. Op basis van een landelijk model is hiervan in 2011 de leesbaarheid vergroot en de lengte gehalveerd. Daarnaast zijn er in de afgelopen jaren een groot aantal beleidsstukken over deelonderwerpen vastgesteld.

Het rapport Cyberdreigingsbeeld[5] van SURF eind 2014 geeft onderwijs- en onderzoeks-instellingen inzicht in de belangrijkste bedreigingen in cybersecurity en privacy. Het helpt cybersecurity en privacy intern hoog op de agenda te zetten en biedt handvatten om de juiste maatregelen te nemen om aanwezige informatie veilig, betrouwbaar en toegankelijk te houden.

Winter 2014-2015 is samen met vertegenwoordigers vanuit de faculteiten en ICTS het informatiebeveiligingsbeleid geëvalueerd en herzien. Hierbij is veel tijd besteed aan het formuleren van een set basisregels, die kort uitdrukken wat we als UT echt belangrijk vinden.

1.4 Leeswijzer

De aparte hoofdstukken in dit beleidsdocument zijn zelfstandig leesbaar. Er worden normen geformuleerd die implementatie behoeven door de betreffende verantwoordelijken. Alle lezers wordt aangeraden in ieder geval uit hoofdstuk 3 Uitgangspunten de paragraaf 3.1 Basisregels en 3.2 Beleidsuitgangspunten door te lezen. In hoofdstuk 4 over Governance wordt expliciet geformuleerd hoe de verantwoordelijkheden op de UT met betrekking tot informatiebeveiliging belegd zijn. De rollen van security officer, security manager en CERT-UT (Computer Emergency Respons Team) worden hier vastgelegd.

In de bijlagen wordt ingegaan op de relevante wetgeving en worden de securityregels (operationele richtlijnen) geformuleerd. Voor de evaluatie en bijstelling van deze vrij technische securityregels zijn betreffende ICTS-medewerkers intensief betrokken. Door deze securityregels op te nemen als bijlage is de relatie tussen de securityregels en het beleid helder. De securityregels zijn zo geformuleerd dat ze ook begrijpelijk zijn voor niet-technici. ICTS-medewerkers die alleen geïnteresseerd zijn in de consequenties voor hun eigen werk kunnen volstaan met het lezen van de betreffende securityregels.

[5] Rapport Cyberbedreigingsbeeld Sector Hoger Onderwijs en Wetenschappelijk Onderzoek https://www.surf.nl/kennis-en-innovatie/kennisbank/2014/rapport-cyberbedreigingsbeeld-sector-hoger-onderwijs-en-wetenschappelijk-onderzoek.html

2 Doelstelling informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid bij de UT heeft als doel het waarborgen van de continuïteit van bedrijfsvoering, onderwijs en onderzoek en het minimaliseren van de schade door het voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen.

De doelen van het informatiebeveiligingsbeleid voor de UT zijn meer specifiek de volgende:

- *Kader*: het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan een vastgestelde best practice of norm en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.
- *Normen*: de basis voor de inrichting van het security management is ISO 27001.[6] Maatregelen worden genomen op basis van best practices in het hoger onderwijs en o.b.v. ISO 27002[7].
- *Expliciet*: uitgangspunten en organisatie van informatiebeveiligingsfuncties zijn vastgelegd en worden gedragen door het College van Bestuur, en afgeleid daarvan, door de hele organisatie.
- *Daadkrachtig*: basis voor duidelijke keuzes in maatregelen, actieve controle op beleidsregels en de uitvoering daarvan.
- *Compliance*: het beleid biedt de basis om te voldoen aan wettelijke voorschriften.

[6] Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging
[7] Voluit: NEN-ISO/IEC 27002: Code voor Informatiebeveiliging

3 Uitgangspunten informatiebeveiliging

3.1 Basisregels

Algemene strategiedocumenten zoals Vision2020 geven op zichzelf onvoldoende aanknopingspunten om een Informatiebeveiligingsbeleid op te baseren, oftewel om een bij de UT passende risicoacceptatie te formuleren. Om te voorkomen dat het beleid onvoldoende gekend en gedragen wordt door de organisatie is het belangrijk expliciet te formuleren wat we echt belangrijk vinden.

1. *De UT houdt zich, als publiekrechtelijke organisatie, aan de wet.* Volgens velen is dit een open deur. Ook als ondernemende universiteit gaat de UT niet mee in de redenering dat de keuze om je als organisatie aan de wet te houden een kosten-baten analyse hoort te zijn. Anderzijds is de universiteit natuurlijk ook geen politieagent.
2. *Informatie over studenten en medewerkers wordt zo zorgvuldig als mogelijk behandeld.* Aankomende en huidige studenten moeten er op kunnen vertrouwen dat er zo zorgvuldig als mogelijk met hun informatie wordt omgegaan. Deze informatie is voor een groot deel studie-gerelateerd. Zorgvuldig met privacy omgaan is een van de uitdagingen waar we als universiteit voor staan.
3. *Aandacht besteden aan informatiebeveiliging binnen alle processen en activiteiten hoort bij de proactieve houding van de UT-medewerker.* Informatiebeveiliging heeft veel aspecten en raakt aan bijna alle processen en activiteiten. Risico nemen hoort bij de ondernemende houding van de UT. Onderdeel hiervan is vooraf de mogelijke gevolgen te onderzoeken en maatregelen te nemen die onaanvaardbare risico's beperken.
4. *Het ondernemende en creatieve karakter van de UT wordt niet gefrustreerd door het informatiebeveiligingsbeleid.* Noodzakelijke beveiligingsmaatregelen moeten natuurlijk genomen worden, ook als individuen dit minder waarderen, maar dan wel na een afweging. Proportionaliteit is hierbij gewenst. Ingrijpende of beperkende maatregelen die niet in verhouding staan tot het feitelijk verminderen van risico's worden niet genomen.

3.2 Beleidsuitgangspunten

Security management wordt als proces ingericht. Dat houdt in dat de jaarlijkse planning en controlecyclus, gebaseerd is op ISO 27001[8] (Plan, Do, Check, Act). Hierin worden jaarplannen opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen.

De beveiliging dient de volgende aspecten van de informatievoorziening te waarborgen:

- **B**eschikbaarheid: de mate waarin gegevens of functionaliteit op de juiste momenten en locaties beschikbaar zijn voor gebruikers;
- **I**ntegriteit: de mate waarin gegevens of functionaliteit juist ingevuld zijn;
- **V**ertrouwelijkheid: de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

De Universiteit Twente hanteert de volgende beleidsprincipes:

- Informatiebeveiliging is **ieders verantwoordelijkheid**. Communiceer met medewerkers, studenten, docenten en derden dat er van hen verwacht wordt dat ze actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. Dat kan bijvoorbeeld in de aanstellingsbrief, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

[8] Aangezien ICTS ITIL hanteert is het gebruik van ITIL Security Management voor ICTS aangewezen, daar deze is gebaseerd op ISO 27001 en de relatie met de andere ITIL processen uitwerkt.

- Informatiebeveiliging is een **lijnverantwoordelijkheid**. Dit betekent dat de leidinggevenden de primaire verantwoordelijkheid dragen voor een goede informatiebeveiliging op hun afdeling / eenheid. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan.
- Informatiebeveiliging is een **continu proces**. Regelmatige herijking van beleid en audits, technologische en organisatorische ontwikkelingen binnen en buiten de instelling maken het noodzakelijk om periodiek te bezien of de UT nog wel op de juiste wijze bezig is de beveiliging te waarborgen. De audits maken het mogelijk het beleid en de genomen maatregelen te controleren op efficiency en effectiviteit (**controleerbaarheid**).
- **Eigendom van informatie**. De UT is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd, tenzij dit voor bijvoorbeeld onderzoek anders is overeengekomen. Daarnaast beheert zij informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en studenten dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van deze informatie.
- **Waardering van informatie**. Iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. Classificatie kan hierbij behulpzaam zijn; zie de volgende paragraaf.

3.3 Classificatie

Voor het goed functioneren van de Universiteit Twente is het omgaan met informatie van levensbelang. Studenten en medewerkers moeten er op kunnen vertrouwen dat informatie toegankelijk is wanneer en waar die nodig is, correct en volledig is en alleen beschikbaar is voor daartoe geautoriseerde personen.

Niet alle informatie is vertrouwelijk. Het is niet gebruiksvriendelijk om niet vertrouwelijke informatie net zo streng te beschermen als hoog vertrouwelijke informatie. Proportionaliteit, ook omwille van efficiënt gebruik van de beschikbare financiële middelen, is hierbij gewenst. Het ligt voor de hand om onderscheid in bescherming aan te brengen. Classificatie van informatie is hiervoor het hulpmiddel.

Bij de Universiteit Twente zijn alle gegevens, waarop dit informatiebeveiligingsbeleid van toepassing is, geclassificeerd op de kwaliteitsaspecten *Beschikbaarheid*, *Integriteit* en *Vertrouwelijkheid*.

Welk niveau van beveiligingsmaatregelen geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. Voor de classificatie wordt per kwaliteitsaspect de driepuntschaal *Standaard*, *Gevoelig*, *Kritiek* gebruikt.

De classificatie dient door of namens de eigenaar van de betreffende informatie of van het betreffende informatiesysteem te worden bepaald. Voor de instelingssystemen van de UT zijn door het College van Bestuur houders (directeuren van diensten) aangewezen die de rol van eigenaar vervullen. Voor de beschrijving en uitwerking van de beveiligingsniveaus wordt verwezen naar de Classificatierichtlijn Informatie en Informatiesystemen Universiteit Twente,[9] waarin tevens de classificatiemethodiek is geformuleerd.

[9] Classificatierichtlijn Informatie en Informatiesystemen Universiteit Twente, kenmerk SECR/IM/11/0412/khv, zie http://www.utwente.nl/uim/informatiebeveiliging/classificatierichtlijn-ut.pdf

4 Governance informatiebeveiligingsbeleid

Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term *governance*. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de instelling, zoals de studenten, medewerkers en de samenleving als geheel. Een goede *governance* zorgt er voor dat alle belanghebbenden hun rechten en plichten kennen en er naar handelen.

4.1 Afstemming met aanpalende beleidsterreinen

Onderdeel van governance is dat aan alle soorten risico's en hun onderlinge verwevenheid passende aandacht geschonken wordt, dit wordt Integrale Veiligheid genoemd. Fysieke beveiliging, Arbo- en milieuveiligheid blijven hier verder buiten beschouwing.

De problematiek rond privacy, het zorgvuldig verwerken van persoonsgegevens, is onderdeel van informatiebeveiliging. Tegelijkertijd heeft het zoveel specifieke elementen dat hier eind 2015 een apart beleid voor wordt opgesteld.

Bedrijfscontinuïteit valt deels binnen het domein van informatiebeveiliging, maar is primair een lijnverantwoordelijkheid. Eenheden dienen bedrijfscontinuïteitsplannen op te stellen voor de bedrijfsprocessen waar ze verantwoordelijk voor zijn.

4.2 Documenten

Een overzicht van de huidige beleidsdocumenten op het gebied van informatiebeveiliging is opgenomen in Bijlage B. Alle beleidsdocumenten worden na vaststelling gepubliceerd op de website van UIM.[10]

Om de noodzakelijke beveiligingseisen en –procedures vast te kunnen leggen zijn op deelgebieden specifieke securityregels noodzakelijk. Een opsomming van de Securityregels is opgenomen in Bijlage C. Door het formeel vaststellen van deze securityregels wordt de implementatie van het informatiebeveiligingsbeleid toetsbaar.

Algemene voorlichting over informatiebeveiliging wordt door ICTS verzorgd. Specifieke werkinstructies worden in de lijn aan medewerkers verstrekt.

In alle overeenkomsten met dienstverleners is een paragraaf over informatiebeveiliging opgenomen.

4.3 Organisatie van de informatiebeveiligingsfunctie

Informatiebeveiliging is onverbrekelijk verbonden met de informatievoorziening. Buiten enkele specifieke functies, die hierna worden besproken, valt de governance dan ook samen met de IT-governance zoals besproken in "Werk maken van vraaggestuurde ICT en informatie-voorziening."[11] Wat betreft de benaming van de informatiebeveiligingsfuncties wordt zoveel mogelijk aangesloten bij het PvIB.[12]

De *Information Security Officer* is een rol op **strategisch** (en tactisch) niveau binnen Universitair Informatie Management. UIM adviseert na afstemming met het servicecentrum ICTS en eventueel houders van betreffende informatiesystemen aan het College van Bestuur. De Security Officer bewaakt op het gebied van informatiebeveiliging de implementatie van het informatiebeveiligingsbeleid binnen de instelling.

[10] www.utwente.nl/uim
[11] Werk maken van vraaggestuurde ICT en informatievoorziening, kenmerk SB/UIM/12/0915/evs, zie http://www.utwente.nl/uim/it-governance/vraagsturing-ict-informatievoorziening.pdf
[12] Functies in de informatiebeveiliging. Platform voor Informatiebeveiliging (PvIB), 2006

De *Information Security Manager* is een functionaris bij ICTS en vervult een rol bij de vertaling van de strategie naar **tactische** (en operationele) plannen. Bij de diensten ligt deze verantwoordelijkheid bij de systeemhouder die de taak doorgaans heeft gedelegeerd aan het *hoofd functioneel beheer*. Bij de faculteiten ligt deze verantwoordelijkheid bij de facultaire portefeuillehouder ICT.

Op **operationeel** niveau wordt overlegd met ICTS-medewerkers en met functioneel beheerders, onder andere over de implementatie van de informatiebeveiligingsmaatregelen. De Information Security Manager is coördinator van het *CERT-UT* (Computer Emergency Response Team UT).

De beveiliging van informatiesystemen, inclusief de kosten daarvan, zijn een integraal onderdeel van verantwoord beheer van het betreffende informatiesysteem. Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten. Voorlichting en training voor specifieke toepassingen of doelgroepen worden uit decentrale middelen betaald.

4.3.1 College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging binnen de Universiteit Twente en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is gemandateerd aan de Information Security Officer. Deze heeft de opdracht om voor de informatiebeveiliging voor de gehele instelling zorg te dragen.

4.3.2 Portefeuillehouder informatiebeveiliging

De portefeuillehouder informatiebeveiliging is het Collegelid dat ICT in portefeuille heeft. Hij is eindverantwoordelijk voor informatiebeveiliging binnen de Universiteit Twente.

4.3.3 Information Security Officer

De Information Security Officer maakt deel uit van Universitair Informatie Management en functioneert op strategisch en tactisch niveau. Hij adviseert samen met het hoofd Informatie-management het CvB. De Information Security Officer formuleert het informatiebeveiligings-beleid, helpt bij een juiste vertaling daarvan naar instellingsonderdelen, ziet toe op de (uniforme) naleving ervan en rapporteert over lacunes, inconsistenties en onvolkomenheden. Jaarlijks wordt er een securityjaarverslag ten behoeve van het CvB opgesteld.

4.3.4 Information Security Manager

De Information Security Manager functioneert binnen ICTS en vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doet hij in overleg met de Information Security Officer. Hij coördineert het CERT (Computer Emergency Response Team) van de UT. Tevens adviseert hij over specifieke informatiebeveiligingsmaatregelen in projecten – variërend van allerhande staande projecten tot acquisities van bijvoorbeeld software of hardware. Ieder kwartaal wordt er een managementrapportage opgesteld voor de Information Security Officer, het hoofd Informatiemanagement en het ICTS-MT.

4.3.5 Systeemhouder

De systeemhouder[13] is er verantwoordelijk voor dat de applicatie een goede ondersteuning biedt aan de bedrijfsprocessen waarvoor de systeemhouder verantwoordelijk is. Dit betekent dat de systeemhouder er voor zorgt dat zowel nu als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers, aan wet- en regelgeving en aan het informatiebeveiligingsbeleid.

De systeemhouder kan hierin ondersteund worden door de Information Security Officer.

[13] zie verder de notitie “Houderschap van een instellingssysteem”, kenmerk SB/UIM/15/2801/EVS, http://www.utwente.nl/uim/it-governance/houderschap-van-een-instellingssysteem.pdf

4.3.6 Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van (de voor hen relevante aspecten van) het beveiligingsbeleid;
- toe te zien op de naleving van het beveiligingsbeleid door zijn medewerkers;
- regelmatig het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

De leidinggevende kan hierin ondersteund worden door de Information Security Manager en de Information Security Officer.

4.3.7 Functionaris gegevensbescherming

De functionaris voor de gegevensbescherming (FG) houdt binnen de Universiteit Twente toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

4.4 Naleving en bewustwording

De naleving is geborgd met algemeen toezicht op de dagelijkse praktijk van het security management proces. Van belang hierbij is dat leidinggevenden hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen.

De Information Security Officer monitort in hoeverre de organisatie het informatiebeveiligings-beleid heeft geïmplementeerd. Het Normenkader SURFaudit[14] wordt gebruikt als uitgangspunt voor interne en externe controles. Er wordt niet gestreefd naar ISO 27001/27002 certificering.

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste risicofactor. Daarom worden beveiligingsrisico's en –maatregelen regelmatig onder de aandacht gebracht, zodat kennis van risico's wordt verhoogd en het (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van de uitvoering van het informatiebeveiligingsbeleid zijn regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en derden. Zulke campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met beveiligingscampagnes voor Arbo, milieu en fysiek.

Verhoging van het beveiligingsbewustzijn is zowel een verantwoordelijkheid van de leidinggevenden alsook van de Information Security Officer en de Information Security Manager.

4.4.1 Implementatiewerkgroep

Om bewustwording en gedragsbeïnvloeding van medewerkers en studenten met betrekking tot informatiebeveiliging en privacy te bewerkstelligen wordt vanuit Universitair Informatiemanagement een werkgroep ingesteld. De werkgroep stelt een Plan van Aanpak op en heeft in ieder geval de volgende leden:

- Information Security Officer (UIM)
- Information Security Manager (ICTS)
- Beleidsmedewerker HR (HR)
- Communicatiemedewerker (M&C)

[14] Het normenkader van SURFaudit is gebaseerd op ISO 27002.

5 Melding en afhandeling van incidenten

Incidentbeheer en –registratie hebben betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door de medewerkers en studenten gemeld worden en de wijze waarop deze worden afgehandeld.

Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. Bij de Universiteit Twente is er daarom een meldpunt ingericht en is bekend gemaakt hoe dat is te benaderen: CERT-UT, het Computer Emergency Response Team UT.

Elke eenheid is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging. De lijnmanager, medewerker of student dient de incidenten en inbreuken direct te melden aan cert@utwente.nl of via de centrale ICTS servicedesk.

Er is een, door het CvB vastgesteld, responsible disclosure beleid. Daarmee geeft de UT mogelijke melders van veiligheidsgaten in onze informatiesystemen een garantie dat de UT, onder voorwaarden, geen juridische stappen tegen hen zal ondernemen.

De incidenten worden afgehandeld en worden in het relevante operationeel overleg besproken – en als bedrijfsproces, financiën of goede naam in gevaar zijn, ook in het CvB. Bij constatering van verontrustende trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

Het doel van CERT-UT is het zo mogelijk voorkomen van informatiebeveiligingsincidenten en deze te bestrijden zodra ze zich voordoen en daarmee de continuïteit van de Universiteit Twente te ondersteunen en haar reputatie te beschermen. CERT-UT houdt zich ook bezig met beveiligingsincidenten buiten de Universiteit Twente als daar eigen medewerkers of studenten in enige rol bij betrokken zijn. In zulke gevallen wordt gebruik gemaakt van de diensten van SURFcert, die wereldwijd in verbinding staat met andere CERT's.

De leden van CERT-UT zijn benoemd door de directeur ICTS en opereren in diens opdracht. CERT-UT kan in geval van ernstige incidenten via de directeur ICTS escaleren naar de portefeuillehouder informatiebeveiliging. CERT-UT wordt geleid door de Information Security Manager.

CERT-UT is gerechtigd het tijdelijk isoleren van systeem/netwerkgebruikers, computersystemen of netwerksegmenten te gelasten ten einde haar taak uit te kunnen voeren.

In de specifieke securityregels voor Security Incident- en Eventmanagement wordt een en ander verder uitgewerkt.

Bijlage A Wetgeving

Bij de Universiteit Twente wordt op de volgende wijze omgegaan met relevante wet- en regelgeving. Deze lijst is niet uitputtend.

i. Wet op het Hoger onderwijs en Wetenschappelijk onderzoek

De Universiteit Twente heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd. Daarnaast worden integriteitscodes voor wetenschappelijk onderzoek nageleefd en toegepast.

ii. Wet Bescherming Persoonsgegevens

De Universiteit Twente heeft de wettelijke privacy vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het informatiebeveiligingsbeleid. Naleving van de beveiligingsmaatregelen leidt tot voldoen aan de wet.

Eind 2015 wordt het Privacybeleid verder uitgewerkt.

iii. Archiefwet

De Universiteit Twente houdt zich aan de voorschriften ten aanzien van bewaartermijnen, zoals die bijvoorbeeld in de Archiefwet zijn vastgelegd, en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is periodiek onderdeel van de externe accountantsrapportages.

iv. Auteurswet

De Universiteit Twente verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat de Universiteit Twente het gebruik van software zonder het bezitten van de juiste licenties tegen gaat.

De bibliotheek geeft op haar website praktische informatie hoe met auteursrecht om te gaan. ICTS beheert de software licenties.[15]

v. Telecommunicatiewet

De Universiteit Twente kent geen openbaar deel van het netwerk. Het UT-net is beschikbaar voor een gesloten groep van betrokkenen bij onderwijs en onderzoek en geeft toegang tot daarvoor relevante services. Daarom is de meeste regelgeving uit de Telecommunicatiewet niet van toepassing. De regelgeving omtrent netneutraliteit is van toepassing voor zover het de studentenhuisvesting betreft.

vi. Wet op de inlichtingen- en veiligheidsdiensten

Een wijzigingsvoorstel op de Wiv wordt binnenkort in het parlement behandeld. Wanneer dit voorstel wordt aangenomen, dan krijgen diensten als AIVD en MIVD het recht om dataverkeer van het Internet af te tappen. De consequenties voor de UT zullen, bij voorkeur in SURF verband, uitgezocht moeten worden.

[15] http://www.utwente.nl/uim/voor-eindgebruikers/softwarelicenties_en_de_UT.pdf

vii. Wet Computercriminaliteit

De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet bestaat uit artikelen die op diverse plekken zijn toegevoegd aan het Wetboek van Strafrecht. De extra artikelen gaan over:

- Vernieling en onbruikbaar maken
- Aftappen van gegevens
- *Denial of service*, verstikkingsaanval
- Computervredebreuk
- Wat is computercriminaliteit
- Diensten afnemen zonder betalen
- Malware, kwaadaardige software

Het naleven van dit informatiebeveiligingsbeleid en het implementeren van de securityregels zorgen ervoor dat de UT een basisniveau van beveiliging heeft. Indien er aanvallen op de UT plaatsvinden die die beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal de UT in beginsel aangifte doen. De security manager en security officer adviseren hierover het College van Bestuur – alleen het CvB kan het besluit tot aangifte nemen.

Bijlage B Beleidsdocumenten

Naast het Informatiebeveiligingsbeleid zijn een aantal beleidsdocumenten en gedragscodes op het gebied van informatiebeveiliging geformuleerd. Alle beleidsdocumenten worden na vaststelling gepubliceerd op de website van UIM.[16]

1. *Classificatierichtlijn Informatie en Informatiesystemen Universiteit Twente*.[17] Classificatie van informatie geeft een inschatting van de gevoeligheid en het belang van de informatie en de daarbij horende graad van beveiliging. Het gaat daarbij om de juiste mate van beveiliging, één die past bij de risico's die de informatie loopt.
2. *Gedragscode ICT- en Internetgebruik Universiteit Twente voor medewerkers*[18] *en voor studenten*.[19] De gedragscodes geven de wijze aan waarop bij de Universiteit Twente wordt omgegaan met ICT- en internetgebruik. De codes regelen het verantwoord gebruik van ICT-voorzieningen en internet en de wijze waarop controle op het gebruik plaatsvindt.
3. *Gedragscode ICT-functionarissen Universiteit Twente*.[20] Vanuit hun functie hebben ICT-functionarissen vaak verregaande bevoegdheden binnen informatieverwerkende systemen. Door de tools die hen ter beschikking staan kunnen zij vaak op eenvoudige wijze privacygevoelige informatie verzamelen.
4. *Beleidsregels Identitymanagement Universiteit Twente*.[21] ICTS is als houder verantwoordelijk voor het Identitymanagement (IDM) systeem. Het IDM-systeem zorgt voor de authenticatie van gebruikers voor de informatiesystemen.
5. *Wachtwoordbeleid Universiteit Twente*.[22] Bij de opstelling van de Beleidsregels Identitymanagement Universiteit Twente is ervoor gekozen om een apart wachtwoordbeleid op te stellen waarin alle aspecten opnieuw worden afgewogen en uitgewerkt. De verschillende inzichten worden in dit document belicht.
6. *Autorisatiebeleid Universiteit Twente*.[23] Het toekennen van rechten wie wat mag, noemen we autorisatie. Het Autorisatiebeleid geeft algemene richtlijnen hoe bij informatiesystemen om te gaan met autorisaties.
7. *Ambitieniveau SURFaudit*.[24] In SURF-verband is afgesproken dat de instellingen de SURFaudit uitvoeren om het niveau van de informatiebeveiliging te meten. Het CvB heeft besloten om het ambitieniveau voor de SURFaudit vast te stellen op minstens volwassenheidsniveau 3: Defined Process.

[16] www.utwente.nl/uim
[17] zie http://www.utwente.nl/uim/informatiebeveiliging/classificatierichtlijn-ut.pdf
[18] zie http://www.utwente.nl/uim/voor-eindgebruikers/gedragscode_ict_mw-nl.pdf
[19] zie http://www.utwente.nl/uim/voor-eindgebruikers/gedragscode_studenten.pdf
[20] zie http://www.utwente.nl/uim/informatiebeveiliging/gedragscode-ict-functionarissen.pdf
[21] zie http://www.utwente.nl/uim/beleidsregels-identitymanagement-universiteit-twente.pdf
[22] zie http://www.utwente.nl/uim/wachtwoordbeleid-universiteit-twente.pdf
[23] zie http://www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf
[24] zie http://www.utwente.nl/uim/informatiebeveiliging/ambitieniveau-surfaudit.pdf

Bijlage C Securityregels

Om de noodzakelijke beveiligingseisen en –procedures vast te kunnen leggen zijn op deelgebieden specifieke securityregels noodzakelijk. Door het formeel vaststellen van deze securityregels wordt de implementatie toetsbaar. ICTS-medewerkers kunnen zich over het algemeen beperken tot de voor hun relevante securityregels.

De Securityregels vervangen de Security Policies die in 2008 zijn vastgesteld.

Voor de volgende deelgebieden zijn specifieke securityregels vastgesteld:

1. *Authenticatiemiddelen*, beheer en gebruik van wachtwoorden, software- en/of hardwaresleutels. Zie pagina 16.
2. *Basis ICT-voorzieningen,* zoals email, dataopslag, telefonie en chat. Zie pagina 17.
3. *Datacentra* met de daarin opgestelde servers. Zie pagina 18.
4. *Hardware*, de gehele levenscyclus van aanschaf tot uitfasering. Zie pagina 19.
5. *Informatiesystemen*, de gehele levenscyclus van verwerving tot uitfasering. Zie pagina 20.
6. *Netwerk,* inclusief de actieve netwerkcomponenten zoals routers, switches, hubs, access-points etc. Zie pagina 21.
7. *Security Incident- en Eventmanagement*, werkwijze CERT-UT en afhandeling van beveiligingsincidenten. Zie pagina 22.
8. *Werkplekken* van gebruikers. Zie pagina 23.

Securityregels – Authenticatiemiddelen

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft het beheer en gebruik van authenticatiemiddelen. Om toegang te krijgen tot het gebruik van bepaalde ICT-voorzieningen wordt voor de authenticatie naast de gebruikersnaam gebruik gemaakt van een wachtwoord, software- en/of hardwaresleutel.

In de Gedragscode ICT- en Internetgebruik[25], Beleidsregels Identitymanagement, Wachtwoordbeleid en het Autorisatiebeleid worden aanverwante relevante uitspraken gedaan, deze worden hier niet herhaald.

Verantwoordelijkheid

1. ICTS is verantwoordelijk voor de authenticatiemiddelen.
2. Voor alle soorten authenticatiemiddelen bestaat er een auditbare procedure voor uitgifte, gebruik, vervanging, inname en verlies.

Doelbinding

3. Authenticatiemiddelen zijn persoonsgebonden, apparaatgebonden of applicatiegebonden.
4. Persoonsgebonden authenticatiemiddelen zijn persoonlijk en niet overdraagbaar.
5. Voor alle apparaatgebonden en applicatiegebonden authenticatiemiddelen is steeds één persoon verantwoordelijk. Hij beheert het betreffende middel en ziet toe op het gebruik. ICTS registreert wie voor welk authenticatiemiddel verantwoordelijk is.

Wachtwoorden

6. Voor persoonsgebonden wachtwoorden is een zekere mate van complexiteit noodzakelijk. ICTS publiceert een richtlijn die deze eis verder uitwerkt en draagt zorg voor de toepassing hiervan.
7. Apparaatgebonden en applicatiegebonden wachtwoorden zijn zeer complex en hebben een hoge entropie. ICTS publiceert een richtlijn die deze eis verder uitwerkt en draagt zorg voor de toepassing hiervan.
8. Default wachtwoorden zoals ingesteld door de leverancier dienen te worden aangepast.

[25] zie voor de genoemde documenten de UIM website http://www.utwente.nl/uim

Securityregels – Basis ICT-voorzieningen

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de basis ICT-voorzieningen zoals email, dataopslag, telefonie en chat. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. Voor de centraal aangeboden basis ICT-voorzieningen is ICTS houder en verantwoordelijk voor naleving van de securityregels.
2. Voor het veilig gebruik van ICT-voorzieningen geeft ICTS voorlichting op de website.

Uitgifte

3. Bij uitgifte van een account wordt de gebruiker meteen geïnformeerd over security, o.a. door te wijzen op de Gedragscode ICT- en internetgebruik.[26]

Data

4. Toegang tot data, inclusief berichten, configuratie en metadata, van een gebruiker mag alleen met toestemming van de betreffende gebruiker of in schriftelijke opdracht van het CvB, zoals vastgelegd in de Gedragscode. In alle gevallen wordt deze toegang geregistreerd.
5. Alle transport van data voldoet qua versleuteling aan de maatregelen uit de Classificatierichtlijn.[27]

Mail

6. Van alle mail die door de UT wordt verstuurd, dient de persoon of applicatie die de mail heeft verstuurd achterhaalbaar te zijn.
7. In- en uitgaande mail wordt gecontroleerd op malware en spam, zo nodig wordt de mail geheel of gedeeltelijk verwijderd of apart gezet.
8. Het aantal geadresseerden en de grootte van mails zijn aan een redelijke bovengrens gebonden. De details worden door ICTS op de website gepubliceerd.

[26] Gedragscode ICT- en internetgebruik,
zie http://www.utwente.nl/uim/voor-eindgebruikers/gedragscode_ict_mw-nl.pdf
[27] Classificatierichtlijn Informatie en Informatiesystemen,
zie http://www.utwente.nl/uim/informatiebeveiliging/classificatierichtlijn-ut.pdf

Securityregels – Datacentra

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de datacentra met de daarin opgestelde servers. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. ICTS is verantwoordelijk voor de datacentra, inclusief noodstroom, koeling, etc.
2. ICTS maakt sluitende afspraken met leveranciers, zoals FB en SURFnet.
3. ICTS is verantwoordelijk voor de eigen servers in de datacentra en maakt sluitende afspraken met de eigenaren van de overige servers.

Toegang

4. Toegang tot de datacentra is alleen toegestaan voor het plaatsen, onderhouden, vervangen of verwijderen van hardware en voor onderhoud van de datacentra faciliteit zelf.
5. ICTS stelt nadere richtlijnen op voor de toegang tot de datacentra overeenkomstig het Autorisatiebeleid.[28]
6. Alle toegang tot de datacentra wordt geregistreerd.

Servers

7. ICTS houdt een registratie bij van alle geplaatste servers, van iedere server is het doel, een beheerder en een plaatsvervanger geregistreerd. Een registratienummer is goed leesbaar aangebracht op de server.
8. Processen en poorten die niet noodzakelijk zijn voor het gebruik van de server zijn uitgeschakeld.
9. Een server die het UT-net of andere ICT-diensten verstoort of anderszins een securityissue veroorzaakt, wordt op last van CERT-UT uitgeschakeld of geïsoleerd.

Beheer

10. Technisch beheer van applicaties en servers vindt plaats via een netwerk dat logisch gescheiden is van het netwerk voor gebruikers.
11. Voor het beheer wordt gebruik gemaakt van aparte persoonsgebonden beheeraccounts.
12. Gebruik van beheeraccounts wordt gelogd.
13. Beheer van beheeraccounts volgt het Autorisatiebeleid.

[28] http://www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf

Securityregels – Hardware

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de levenscyclus van hardware, van aanschaf tot uitfasering. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. De houder of eigenaar van een systeem is ook verantwoordelijk voor de hardware en voor naleving van de securityregels.
2. Wanneer ICTS het technisch beheer voert, dan is ICTS ook verantwoordelijk voor naleving van deze regels.
3. Wanneer een informatiesysteem op infrastructuur van ICTS draait dan is niet de houder of eigenaar van dat informatiesysteem, maar ICTS verantwoordelijk voor de hardware.

Aanschaf

4. Voor alle hardware die met het UT-netwerk verbonden kan worden is een zekere mate van beveiliging noodzakelijk. De security manager beheert deze minimumvereisten en publiceert deze op de ICTS-website.
5. Wanneer veel of belangrijke hardware wordt aangeschaft dan wordt de security manager tijdig betrokken bij het inkooptraject.

Beheer

6. Default wachtwoorden zoals ingesteld door de leverancier dienen te worden aangepast.
7. Bij incidenten dient de verantwoordelijke aanspreekbaar te zijn. Daartoe registreert ICTS alle hardware die met het UT-netwerk wordt verbonden, c.q. logt het account waarmee toegang verkregen wordt tot het UT-netwerk.
8. Als een firmware-update een securityissue oplost dan moet deze binnen redelijke termijn uitgevoerd worden.

Uitfasering

9. Bij buitengebruikstelling en afvoer van datadragers, zoals harde schijven, tapes, mobiele devices, USB-sticks etc., dienen de gegevens door of namens de eigenaar adequaat vernietigd te worden. ICTS geeft via de website per soort datadrager voorlichting over de wijze waarop dit mogelijk is.

Securityregels – Informatiesystemen

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de levenscyclus van informatiesystemen, van verwerving tot uitfasering. Deze regels worden in dit document vastgelegd. Software aangeschaft voor individuele gebruikers waarbij Beschikbaarheid, Integriteit en Vertrouwelijkheid niet van belang zijn, is niet gebonden aan deze regels.

Verantwoordelijkheid

1. De houder[29] of eigenaar van een informatiesysteem is verantwoordelijk voor naleving van de securityregels.
2. Wanneer ICTS het technisch en/of applicatie beheer voert, dan worden er in de SLA met de houder ook afspraken vastgelegd ten aanzien van de security en de naleving van deze regels.
3. Toegang tot een informatiesysteem wordt geregeld conform het Autorisatiebeleid.[30]

Verwerving

4. Voor of aan het begin van het project wordt er conform de Classificatierichtlijn Informatie en Informatiesystemen[31] een classificatie uitgevoerd, zodat de resultaten nog de vereisten voor het informatiesysteem kunnen meebepalen.
5. Bij het gebruik van cloudservices wordt het Juridisch normenkader cloudservices hoger onderwijs[32] van SURF toegepast.
6. Bij ieder projectplan voor softwareaanschaf of –ontwikkeling wordt een beveiligingsparagraaf opgenomen. De security manager beheert een generiek overzicht van aandachtspunten voor deze paragrafen en publiceert deze op de ICTS-website.

Beheer

7. Bij door de UT ontwikkelde software worden security issues opgelost.
8. Patches en updates van leveranciers worden planmatig uitgevoerd.
9. Functiescheiding wordt daar waar nodig toegepast, voorbeeld: ontwikkelaars hebben geen rechten op de productieomgeving.

Logging

10. Er wordt niet meer gelogd dan noodzakelijk.
11. De houder houdt een registratie bij van de doelen en bewaartermijnen van de logfiles van alle informatiesystemen onder zijn verantwoordelijkheid.

Uitfasering

12. Niet meer ondersteunde software wordt uitgefaseerd, tenzij dit niet mogelijk is en passende maatregelen securityrisico's voldoende beperken.
13. Bij uitfasering wordt aandacht besteed aan conversie, archivering en vernietiging van data.

---

[29] zie ook http://www.utwente.nl/uim/it-governance/houderschap-van-een-instellingssysteem.pdf
[30] zie http://www.utwente.nl/uim//informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf
[31] zie http://www.utwente.nl/uim/informatiebeveiliging/classificatierichtlijn-ut.pdf
[32] zie https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/juridisch-normenkader-cloudservices-hoger-onderwijs.pdf

Securityregels – Netwerk

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft het netwerk inclusief de actieve netwerkcomponenten zoals routers, switches, hubs, access-points etc. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. ICTS is verantwoordelijk voor het netwerk, inclusief alle actieve netwerkcomponenten zoals routers, switches, hubs, access-points etc.
2. Actieve netwerkcomponenten worden voor zover mogelijk in een afgesloten ruimte geplaatst.
3. ICTS houdt een registratie bij van alle actieve netwerkcomponenten.
4. De UT hanteert als uitgangspunt een open netwerk waar in beginsel geen beperkingen aan internetverkeer worden opgelegd.
5. De UT houdt zich aan de afspraken zoals die gemaakt zijn met SURFnet.

Eigen apparatuur

6. In principe verzorgt alleen ICTS de plaatsing van netwerkapparatuur. ICTS houdt een registratie bij van de uitzonderingsgevallen inclusief de gemaakte schriftelijke afspraken.
7. ICTS houdt een registratie van derdenaansluitingen bij, met vastlegging van de gemaakte afspraken.
8. Apparatuur die het UT-net of andere ICT-diensten verstoort of anderszins een securityissue veroorzaakt, wordt op last van CERT-UT uitgeschakeld of geïsoleerd. Dit geldt ook voor apparatuur die het gebruik van het draadloze netwerk verstoort.

Campus

9. Campusbewoners mogen eigen routers etc. installeren.
10. Wanneer de router van een campusbewoner of een van de systemen achter de router het UT-net of andere ICT-diensten verstoort of anderszins een securityissue veroorzaakt, wordt op last van CERT-UT de router uitgeschakeld of geïsoleerd.

Beheer

11. Beheer van netwerkcomponenten vindt plaats via een gescheiden beheernetwerk of tenminste via een beveiligde verbinding.
12. Beheertoegang tot netwerkcomponenten wordt geregeld conform het Autorisatiebeleid.[33]

[33] zie http://www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf

Securityregels – SIEM (Security Incident- en Eventmanagement)

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de werkwijze van CERT-UT en de afhandeling van beveiligingsincidenten. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. ICTS is verantwoordelijk voor het inrichten en functioneren van CERT-UT zoals vastgelegd in het Informatiebeveiligingsbeleid.
2. De security manager is verantwoordelijk voor het Security Incident- en Eventmanagement.

Incidenten

3. Incidenten worden onmiddellijk via de ICTS-Helpdesk of rechtstreeks aan CERT-UT gemeld.
4. CERT-UT hanteert standaard procedures voor het registreren en verhelpen van incidenten.
5. Er is een specifieke procedure voor securitycalamiteiten.
6. Alle meldingen worden vertrouwelijk behandeld.

Events

7. Acties, handelingen of gebeurtenissen die invloed kunnen hebben op de beveiliging van informatie worden geconstateerd en geregistreerd. Wanneer een event invloed heeft op de bedrijfsvoering dan wordt dit als incident gemeld.

Preventie

8. De security manager geeft voorlichting aan gebruikers, ontwikkelaars en beheerders om securityincidenten te voorkomen.
9. De security manager kan gevraagd en ongevraagd advies uitbrengen over mogelijke beveiligingsproblemen.

Rapportage

10. De security manager levert ieder kwartaal een managementrapportage over de geconstateerde incidenten, events en uitgebrachte adviezen aan de security officer.
11. Deze rapportage behandelt in ieder geval alle securitycalamiteiten en gesignaleerde trends.

Securityregels – Werkplekken

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de werkplekken van gebruikers. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. ICTS is verantwoordelijk voor de beveiliging van werkplekken voor zover die door ICTS worden beheerd.
2. Gebruikers zijn verantwoordelijk voor de beveiliging van hun eigen werkplek voor zover die niet door ICTS wordt beheerd. Via de ICTS website kunnen ze beveiligingsinformatie en –hulpmiddelen vinden.

Beheer

3. Voor het beheer door ICTS wordt gebruik gemaakt van aparte persoonsgebonden beheeraccounts.
4. Gebruik van beheeraccounts wordt gelogd.
5. Beheer van beheeraccounts volgt het Autorisatiebeleid.[34]

Gebruikers

6. Medewerkers vragen nooit aan gebruikers om het wachtwoord af te geven. Zo nodig wordt gevraagd om in te loggen.
7. Gebruikers worden door ICTS periodiek actief geïnformeerd over beveiliging, hierbij wordt o.a. gewezen op de Gedragscode ICT- en internetgebruik.[35]

Storingen

8. Een werkplek die het UT-net of andere ICT-diensten verstoort of anderszins een securityissue veroorzaakt, wordt op last van CERT-UT uitgeschakeld of geïsoleerd.

[34] zie http://www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf
[35] Gedragscode ICT- en internetgebruik,
zie http://www.utwente.nl/uim/voor-eindgebruikers/gedragscode_ict_mw-nl.pdf